Federal Emergency Management Agency

Washington, D.C. 20472

January 27, 1999

Jacob J. Lew
Office of Management and Budget
Old Executive Office Building
Washington, DC 200

Dear Mr. Lew:

Enclosed is the Electronic Commerce-Implementation Plan for the Federal Emergency management Agency (FEMA). We have divided our plan into three sections as requested in your November 25, 1998 memorandum. The first section is broken down into six blocks and addresses the major initiatives planned for FY1999 and FY2000. Following that section is FEMA's EC Implementation Plan including a list of tasks anticipated completion dates, an architectural chart of the buying and paying process. The third section covers FEMA's management structure and processes. We have tied this plan to our GPRA measures as well as the Information Technology (IT) and Financial Management (FM) 5-year strategic plans.

As a disaster response Agency it is critical that we maintain the most efficient acquisition process available and to stay current. Throughout the implementation of this endeavor, industry standards will be followed. We have drawn on the expertise of Acquisition, Financial Management and Information Technology personnel to help identify and prevent roadblocks. The approach we have to take is to plan for change. The process of developing this plan has laid the groundwork for an agency electronic commerce system,

Questions, concerning this plan, can be directed to Mary O'Donovan of the Grants and Acquisition Support Division on 202-646-4588.

Sincerely,

Gary D. Johnson

Electronic Commerce Implementation Plan

## I.	Major Initiatives

A.	Contract Formation/Administration
B.	Electronic Catalogs
C.	Contract Writing Systems
D.	Payments Utilities
E.	ID and Authentication
F.	Federal System Interfaces

## II.	Milestones and Measurements

## III.	Management Structures and Processes

### A.	Contract Formation/Administration

The FEMA acquisition staff have available state-of-the-art procurement related automation tools to perform contract formation and administration. The Internet is available for contracting personnel to use as a market research tool. We are pursuing the idea of a single-point-of-entry (General Services Administration's Electronic Posting System - EPS) and using the Small Business Administration's PRONet System and other electronic capabilities to improve our Agency's knowledge of sources and services.

FEMA uses an automated software program to formulate, track, and administer procurement actions (ProDoc/ProTrac). In the future, this system will be enhanced with response software. In FY 1999, this system will be interfaced with our financial system (IFMIS). Large procurements have been posted to CBD as well as FEMA's web site in an effort to afford contractors better access to FEMA procurement information with a minimum of effort and cost. Contractors now are able to download solicitations from the FEMA web site and by FY 2000 to submit proposals. During FY 1999, FEMA's policy will be to post all appropriate procurements above $25,000 to our Agency web site and increase the usage of electronic tools for purchasers.

Purchase cards have been issued to over 500 FEMA employees and are used in day-to-day procurements as well as disaster site work. In FY 1998, sales totaled $18.1 million amounting to 2,893 transactions for an average

purchase amount of $890. It is FEMA's policy that program offices procure supplies and services under $2,500 with their purchase card.

This Agency also utilizes many IDIQ contracts to streamline its buying effort. During FY 1999 the Office placed additional emphasis on this area to implement administration electronically. FEMA is in the process of establishing business arrangements with our task order contractors to use the Internet to issue day-to-day transactions.

FEMA has actively implemented procurement reform changes and initiatives including consistently using past performance as an evaluation factor and in contract administration. In an effort to improve our efficiency, the Agency is in the process of identifying and evaluating existing past performance systems and will select a system during FY 1999.

B. Electronic Catalogs/Security

Agency personnel are encouraged to use electronic catalogs using their purchase cards to do micro-purchases and simplified acquisitions. Contracting cardholders also use the Small Business Administrations' electronic PRONet system to search for vendors and link to electronic catalogues. The Agency currently maintains an Intranet site to help purchasers locate electronic catalogues for various products and services available.

FEMA intends to take full advantage of the benefits offered by electronic catalogs and will pursue the idea of partnering with NASA to develop catalog interoperability.

C. Contract Writing Systems

FEMA uses a logic driven, Agency-wide, off-the-shelf contract document generating system (PRODOC). This software package was modified by Distributed Solutions and is continually being updated and improved to meet recent statutory, regulatory and political environment changes.

FEMA's automated procurement system includes a document generation module (ProDoc), a procurement collection, tracking, and reporting module (ProTrac), a regulation search module (RegSearch), and a Dun and Bradstreet business locator> The system supports headquarters, satellite and regional procurement personnel in the acquisition of goods and services to meet Agency mission and goals.

ProDoc and Reg Search are currently loaded on local fileservers at headquarters, satellite and regional procurement offices. Dun and Bradstreet is a yearly software subscription loaded on a headquarter's fileserver that provides access to satellite offices.

ProTrac is the database collection module of the automated procurement system. It is also used to for acquisition strategies, contract administration plans, and close-out. Currently this system is loaded on local fileservers at headquarters and satellite offices and is connected via an enterprise software license on a centralized fileserver except for the regions. Plans are underway to expand this capacity to the regions by FY 2000.

The System has the capability of creating HTML and PDF files for the Agency's internet web site, and many other *tools (Dun and Bradstreet and Reg Search*) to help contract specialist perform and monitor work with less administrative effort.

Prepare and issue award documents – All solicitation and award documents are generated using PRODOC. These files are uploaded to the Agency's internet web site for contractor viewing and downloading. Once electronic signature becomes an effective tool we will be able to send the final award documents over the internet.

D.   Payment Utilities

Electronic Invoicing - FEMA's Integrated Financial Management Information System (IFMIS) is currently being modified by its developer to accept electronic invoices. This interface will be piloted with CitiBank Corporation for purchase card invoicing. Given the nature of the credit card, FEMA and CitiBank have agreed that FEMA will pay CitiBank invoices on a 24-hour turnaround basis to take advantage of rebates offered. This means that the IFMIS, for this first phase, will not include the reconciliation logic necessary to accommodate routine invoices electronically. Development of the second phase will begin shortly after the pilot with CitiBank is declared a success.

Electronic Payments - FEMA has been supporting the ability to pay commercial vendors electronically for several years. In partnership with the Department of Treasury, FEMA transmits encrypted vendor payment data electronically on a daily basis, which is then followed by the transmission, to Treasury, of the payment certification utilizing Treasury's Electronic Certification System (ECS). There are two non-ECS payment file formats currently being utilized in this process. One format is used by Treasury to produce a payment that makes use of the banking system's Automated ClearingHouse (ACH) to electronically deposit payments into a payee's bank account. Modifications to the IFMIS are currently underway to expand the types of formats it uses to produce electronic payments. The other format in use produces a check to be mailed to the payee. The volume of payees receiving checks has been decreasing significantly over the past several months. Additionally, FEMA intends to support and comply with all Federal Government initiatives in this regard and is aggressively collecting the vendor banking information necessary to make these payments electronically.

In concert with Health and Human Services' SMARTLINK system, the IFMIS exports electronic files containing authorizations for States' grants and for the importing of States' drawdown information against those grants.

The new Intra-Governmental Transfer System (IGOTS) is the new intra-agency credit card system used for purchases of supplies between agencies. Work is underway with other agencies to have all intra-agency transactions paid by credit card, including DOD and COE.

E.   **Buyer and Seller ID/Authentication**

FEMA is working to use off-the shelf encryption products where it can and where it can not use an outside server with interface capabilities. Questions still need answers but FEMA is moving to manage the risks involved. FEMA is working with other agencies with common interest to provide a useful infrastructure that is lest costly. The Agency prefers a system, which would assist acquisition, accounting, and logistics to obtain information about vendors to complete their business electronically.

Method in which FEMA addresses security by way of data encryption.

(1) FEMA has had limited requirements to implement data encryption during transmission over public facilities. Primarily these capabilities are "program specific" that include the mandatory use of US Government COMSEC hardware and algorithms. Each device is inventoried and controlled. Only persons with an appropriate clearance have access to this capability.

Capabilities include encryption capabilities for:

- Voice transmission
- Data transmission over voice lines
- Facsimile transmissions
- Point to point video conferencing
- Point to point data over dedicated circuits
- Point to point data over HF radio links

(2) 128 bit public encryption has been implemented on OHRM networks that require access to the National Finance Center. This capability is provided by the addition of a service pack addition to the Microsoft Explorer browser. Connections are established through a dedicated connection connected to the FSN, which also incorporates an Internal firewall to control access.

(3) FEMA has also implemented an electronic certificate that permits personnel that update the FEMA website to authenticate as authorized users. The certificate encrypts the login and passwords. Once permitted access the sessions are not encrypted.

(4) FEMA has implemented a vendor provided capability to manage the external Firewalls remotely. The service is certificate based and uses RSA encryption during the entire remote session.

FEMA is aware of recent discussions to implement data encryption requirements on all data that traverses public networks and/or is stored on devices that can be compromised. At present, standards and guidance have remained unresolved by the Federal working groups responsible for implementing standards. Electronic commerce interactivity with the public will cause FEMA to evaluate and develop standards that follow available Federal standards.

Describe the security methods implemented for our interface with Citibank. Includes any encryption methods used.

Citibank and FEMA have implemented the first Phase of an interface between IFMIS and Citibank's data warehouse.

Current processes included the creation of an FTP (file transfer protocol) directory on FEMA's Internet FTP host. Citibank transfers an accounting file to this directory of credit card accounting then OFM from behind FEMA's firewall logs in and transfers the file manually to IFMIS. The file is not encrypted but compressed in a proprietary Citibank format. Citibank has provided OFM a copy of their proprietary decompress software. The file must be passed through this software to convert it to a usable and readable format.

A second Phase discussed but not in place is to establish an application style server inside of FEMA's firewall that OFM users will access and then the application server will make a dial up connection directly to Citibank's data warehouse. This is a service offered by Citibank. FEMA's network security office has not received complete details required to make an appropriate evaluation of potential threats that maybe introduced by the use of this capability.

Security measures taken in the NEMIS - IFMIS interface.

IT-EN has provided the PMG group with options and suggestions to implement additional security controls in NEMIS. The NEMIS - IFMIS interaction has not been a service identified formally. Recent beta testing and changes in workflow have prevented a complete requirement from being established.

At this time IT-EN has the resources to provide this guidance and awaits a final description of requirements from the PMG office.

FEMA's Firewall (in general terms) and how it is designed to prevent unauthorized users from accessing FEMA resources.

(**1)** FEMA uses "proxy" based firewalls as a security measure to protect unauthorized users from entering the FEMA network trough the dedicated Internet connections. The proxy technology is rules based. An overview of these rules include:

- Only connections initiated from an authorized internal IP address are recognized.
- Internal users are never connected directly to the internet
- Only secured data ports are authorized.
- Internal users IP addresses are not transmitted over the Internet
- Only the external portion of the firewall interacts with the internet
- The external firewall portion retrieves data and passes it to the internal portion of the firewall by use of secured ports, this process is a "proxy".

Each session is recorded in system user logs. Attempts to access services not authorized are denied and recorded in system logs. Attempts by unauthorized users to penetrate the Firewall from the Internet are recorded.

Modems and backdoor maintenance devices are not permitted on the Firewall or any device that is designed to live outside the firewall that could increase the threat of compromising these systems.

(2) A specific Internet firewall and capability was implemented to allow a limited group of users to traverse the firewall and connect to specific internal websites. This capability was in response to requirements to support the RRIS interactions with other Federal Agencies. The add on plug to this firewall is certificate based and allows only those clients issued an electronic certificate to have this capability. All users and their sessions are logged in the system log files. Management of this capability is split between two groups to ensure that a check and balance process exits with independent responsibility and accountability. IT-EN manages the firewall portion, IT-OM manages the certificates for the users.

(3) Internal firewalls have been implemented as a part of the overall network security threat reduction process. These devices provide a DMZ zone between other private networks that connect directly to the FSN. (Eg:) Ex: National Hurricane Center, National Finance Center. These devices provide IP based types of services only with specific rules that restrict and control who and where users can reach between networks. They act much like a fence between neighbors.

As a requirement in FY-99 additional firewalls will be placed in front of critical systems, as an enhancement to security plans, to restrict only authorized internal employees who have a requirement to gain access to these systems.

During FY 1999 the Office of Financial Management will work closely with IT staff to ensure adequate security for electronic acquisition and payment functions. The Agency will continue to assess FEMA's firewall as inter-activity with the public is critical to the successful implementation of the electronic commerce.

F.   Federal Systems Interfaces

Interface Diagram -The attached diagram depicts, at a very high level, FEMA's external financial system's interfaces as they apply to commercial vendors. Depicted are three modes of communication. First, FEMA's Wide Area Network / Local Area Network (WAN/LAN), provides connections between various FEMA operated computer platforms running the IFMIS, the National Emergency Management Information System (NEMIS) and acquisition management's ProTrac/ProDoc contracting applications as well as various PC workstations for the moving around of various interface files. This method provides support in accepting and acknowledging files from the NEMIS, which contain financial transactions related to disaster relief activities. Also supported is the passing of commitment and obligation information between the IFMIS and the systems used by FEMA's acquisition management staff to generate and track contracts with commercial vendors. Second, modem connections allow interface files to be transferred via commercial phone lines utilizing appropriate encryption techniques. An interface utilizing PC workstations is supported by a combination of this method and the aforementioned WAN/LAN technology to provide and track state grant information. Also supported is a host-to-host connection allowing FEMA's IFMIS computer platform to send vendor payment files to Treasury's mainframe computer(s) for disbursement. And third, the intranet / internet connection byway of a FEMA firewall allows for interface files traverse the World-Wide Web. This method supports the electronic invoicing capability now under development and being piloted with CitiBank and acquisition management's process of sending out solicitations to the vendor community and receiving.

II. Milestones and Measures

Enclosed is a chart of all anticipated completion dates of all major initiatives to be completed in FY 1999 and FY 2000 along with those initiatives completed in FY 1998. Also enclosed is a chart of our Acquisition EC implementation plan. We will review our Agency plan every 3 months and monitor all initiatives as they become electronic.

III.   Management Structures and Processes

The Agency actively began testing current electronic commerce activities throughout the procurement process during FY 1998. FEMA is a member of the Interagency Acquisition Internet Council committee. We have participated in several government-wide meetings and workshops to implement Electronic Commerce.   As a member of the Small Agency Council, we have worked with both large and small agencies to determine the most effective implementation plan.

FEMA will continue to collaborate with larger agencies to streamline the procurement process through effective partnerships with others. The Agency's electronic commerce initiative is supported through participation across the Agency with representatives from procurement, financial management and information technology. FEMA also has an Information Resources Board (IRM) that provides a senior-level oversight to the development of the Agency's IT Strategic Plan and promotes the improvement of Agency practices in the modernization, use, sharing, and performance measures.

FEMA's Intranet architecture

FEMA's Intranet is comprised of the FSN.   Primarily it is T-1 (1.544 mbs) dedicated network that connects locations and local area networks, Supported protocols include TCP/IP and IPX/SPX. FEMA has a class B IP addressing design. The network is designed to use core devices as entry points from user locations.

Other highlights include:

- High speed switched LANS (100 - 200 mbs)
- Token based FDDI interfaces (100 mbs)
- Virtual LAN and switching architecture
- Switched Ethernet LANs (10 mbs)
- ATM switching capabilities
- Voice and data over common connections
- Dial Remote access and authentication
- Secure ID used to control access to manage devices
- Network monitoring (HP Openview)
- Network statistics (RMON 2 devices)

FEMA has completed the Financial Management 5-year plan as well as the Information Technology 5-year plan.   Both have incorporated electronic commerce into these plans. These plans and staff members of the respective

offices have participated in the development of the Agency's EC-Implementation Plan. The Agency's EC Coordinator designated to oversee the implementation of this plan is the Chief Financial Officer. Additional Agency representation and coordination will continue between the OFM and IT through the Agency Task Force, Representatives including the designated point of contact, Christine A. Makris, Grants & Acquisition Support Division, Office of Financial Management.

FEMA Electronic Commerce Implementation Plan

	Lead Office	Date
Establish FEMA EC Team	AQ	1998
Develop Agency Implementation Plan	AQ,IT,FM	1999
Develop Pilot Project (Security, Invoicing)	AQ,IT,FM	1999
Implement and Tests Pilots	AQ,IT,FM	1999
Coordinate with Trading Partners	AQ,FM	1999/2000

- Vendor/Trading Partner Initialization
- Notify Current FEMA Vendors to Register
- Establish Vendor/Trading Partner Community

	Lead Office	Date
Review Communications Alternatives	AQ,IT,FM	Ongoing
Define System Requirements (Architecture)	IT	Ongoing

- Hardware
- Common Database Translations Software
- Telecommunications
- Personnel Requirements
- Upgrade Deficient Sites

	Lead Office	Date
Financial Systems Architecture	IT,FM	Ongoing

- Electronic Fund Collections
- Electronic Payment
- Electronic Invoices

	Lead Office	Date
Plan and Budget for Implementing EC	FM	Ongoing
Payment/Acquisition policies and procedures	AQ/FM	Ongoing
Provide Data Requirements to EPIC	AQ	Ongoing
Provide User Training and Guidelines	AQ,IT,FM	1999
Incorporate into existing Agency Management Structure for Upgrading Requirements And Maintenance	AQ,IT,FM	Ongoing
Conduct Project Review and report to Coordinator every 3 months	AQ,IT,FM	Ongoing

Acquisition's Phased Implementation Strategy of Electronic Commerce for Purchasing and Related Activities

PHASES	Completion Date <u>Anticipated</u>

Phase I—Initial Implementation

- *Finalize FEMA's AQ EC Strategic Plan* — 1998
- *Incorporate EPIC EC Milestones* — 1998
  - *Report to EPIC quarterly*
  - *Review final report*
  - *Continue Participation with EPIC Group*
- *Via the FEMA Web Site:* — *1998*
  - Post all suitable RFQ's, draft SOW's, solicitations, amendments, cancellations, and award information
  - Post the Small Business Forecast and the publication 'Doing Business with FEMA'
  - Post and Fax on Demand the List of Active Contractors
  - Maintain an Intranet site for AQ contracting personnel
  - Receive requests for RFP's
  - Vendor Communication via E-Mail
- **Increase and enhance purchase card use** — Ongoing
- **Continue IT coordination (Phase I-IV)** — Ongoing
  Coordinate Agency/private sector EC Outreach to vendors via policy — 1999
- **Maintain a Bulletin Board for Acquisition Management And Grants Management** — 1998

Phase II —Planned Implementation for Pilot Contracts

- **Setup external IT capabilities (Firewall)** — 1999
  - Feasibility Assessment of Server Capabilities)
- *Via the FEMA Web Site:* — 1999
  - Pilot test for Task Order Contracting via FEMA's web site
    - Each division will provide one contract for the pilot
    - Letter to contractor explaining the process
    - Fax copies will be used in lieu of hard copies
    - Automate task order form
- **Regional ProDoc Windows capability** — 1998
- **Initial Regional ProTrac Windows capability** — 1999
- **Evaluate using EC Past Performance sources (i.e., Dun and Bradstreet)** — 1999

Phase III—Initial Final Phase

- **Implementation of Past Performance Systems Capabilityc**   **1999**
- *Via the FEMA Web Site:*   **1998**
    - Receive Responses to RFP's via CBDPlus
    - Evaluate CBDPlus and other sources applicability to FEMA
- **Coordinate Electronic Fund Transfer Payment Process With FM**   **1999**
- **Enhance capability of performance**   **Ongoing**

Phase IV—FY2000—Final Phase

- **Regions fully implemented**   **2000**
- **End to end EC as suitable, practical, and appropriate**   **2000**

NOTE: Satellite and Regional Procurement Offices are included in this process.